(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104781823 B
(45)授权公告日 2018.08.10

(21)申请号 201380060056.X

(22)申请日 2013.11.05

(65)同一申请的已公布的文献号
申请公布号 CN 104781823 A

(43)申请公布日 2015.07.15

(30)优先权数据
12192952.5 2012.11.16 EP

(85)PCT国际申请进入国家阶段日
2015.05.18

(86)PCT国际申请的申请数据
PCT/EP2013/072987 2013.11.05

(87)PCT国际申请的公布数据
WO2014/075944 EN 2014.05.22

(73)专利权人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬

(72)发明人 J-P.M.G.林纳茨

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 王兴秋 景军平

(51)Int.Cl.
G06F 21/32(2006.01)
G06F 21/34(2006.01)

(56)对比文件
US 2006/0274920 A1,2006.12.07,
WO 2010/064162 A1,2010.06.10,
EP 1237091 A1,2002.09.04,
CN 102404328 A,2012.04.04,
Jean-Paul Linnartz等.New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates.《Lecture Notes in Computer Science》.2003,第2688卷第393-402页,图1.

审查员 崔成东

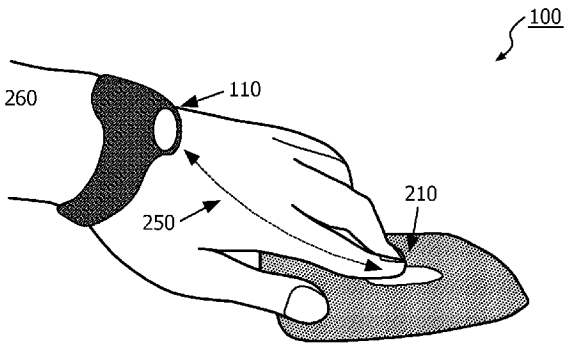
权利要求书2页 说明书12页 附图4页

(54)发明名称

具有身体耦合通信接口的生物计量系统

(57)摘要

一种生物计量系统(100)包括:身份证明系统(110),其包括存储用于个体的生物计量特征的生物计量验证数据的非易失性存储器(125)、以及被配置为凭借身体耦合通信沿着或穿过个体的身体将生物计量验证数据传送到第二身体耦合通信接口的第一身体耦合通信接口(130);以及身份验证系统(210),其包括被配置为测量个体的生物计量特征以获得生物计量数据的生物计量阅读器(220)、被配置为凭借身体耦合通信沿着或穿过个体的身体接收生物计量验证数据的第二身体耦合通信接口(230)(生物计量阅读器被布置为使得所述第二身体耦合通信接口在通过生物计量阅读器(220)对生物计量特征进行测量期间接触或紧靠个体以允许所述接收)、以及被配置为对照生物计量验证数据验证所获得的生物计量数据的生物计量数据验证器。



CN 104781823 B

1.一种身份证明系统(110),包括

- 非易失性存储器(125),其存储特定于个体的生物计量特征的生物计量验证数据,所述生物计量验证数据包括生物计量助手数据以减少来自通过生物计量阅读器(220)获得的生物计量数据的噪声,生物计量阅读器(220)被配置为测量所述个体的生物计量特征,以及

- 第一身体耦合通信接口(130),其被配置为凭借身体耦合通信沿着或穿过所述个体的身体将所述生物计量验证数据传送到第二身体耦合通信接口。

2.一种身份验证系统(210),包括

- 生物计量阅读器(220),其被配置为测量个体的生物计量特征以获得生物计量数据,所获得的生物计量数据受到噪声,

- 第二身体耦合通信接口(230),其被配置为凭借身体耦合通信沿着或穿过所述个体的身体接收生物计量验证数据,所述生物计量阅读器被布置为使得所述第二身体耦合通信接口在通过所述生物计量阅读器(220)对所述生物计量特征进行测量期间接触或紧靠所述个体以允许所述接收,所述生物计量验证数据包括生物计量助手数据,

- 生物计量数据计量器,其被配置为在所述生物计量助手数据的控制下减少来自所获得的生物计量数据的噪声,以及

- 生物计量数据验证器,其被配置为对照所述生物计量验证数据验证所获得的生物计量数据。

3.一种生物计量系统(100),包括

- 根据权利要求1所述的身份证明系统(110),以及

- 根据权利要求2所述的身份验证系统(210),其中所述生物计量阅读器(220)被配置为测量针对其的所述生物计量验证数据被存储在所述非易失性存储器(125)中的所述个体的所述生物计量特征,并且其中所述第二身体耦合通信接口(230)被配置为从所述第一身体耦合通信接口(130)接收所述生物计量验证数据。

4.如权利要求3中所述的生物计量系统,其中所述身份证明系统(110)被包括在腕表中。

5.如权利要求3中所述的生物计量系统,其中所述验证数据包括控制生物计量数据,已预先通过测量所述个体的所述生物计量特征获得所述控制生物计量数据,所述生物计量数据验证器被配置为对照所述控制生物计量数据来验证所获得的生物计量数据。

6.如在权利要求3中所述的生物计量系统,其中所述验证数据包括验证码,通过应用密码学单向函数到控制生物计量数据来预先获得所述验证码,已通过测量所述个体的所述生物计量特征来预先获得所述控制生物计量数据,所述生物计量数据验证器被配置为应用所述密码学单向函数到所获得的生物计量数据以获得候选验证码并且被配置为测试所述候选验证代码是否等于所述验证码。

7.如权利要求3中所述的生物计量系统,其中所述验证数据包括标识所述个体的身份数据,所述身份数据被用于应用中,所述身份验证系统包括被配置为如果所述生物计量数据验证器验证了所述生物计量验证数据则将所述身份数据转发到所述应用的身份输出单元。

8.如权利要求3中所述的生物计量系统,其中所述验证数据包括数字签名,并且所述身份验证系统包括被配置为验证所述数字签名的数字签名验证器,其中所述数字签名对所述

验证数据的至少一部分进行了签名。

9.如权利要求3中所述的生物计量系统，其中个体的所述生物计量特征是所述个体的指纹并且所述生物计量阅读器是指纹阅读器。

10.如权利要求3中所述的生物计量系统，其中

- 所述第二身体耦合通信接口(230)被配置为凭借身体耦合通信沿着或穿过所述个体的身体传送对生物计量验证的请求到所述第一身体耦合通信接口，

- 所述身份证明系统(110)被配置为响应于凭借身体耦合通信沿着或穿过所述个体的身体接收所述对生物计量验证的请求，来凭借身体耦合通信沿着或穿过所述个体的身体传送生物计量验证数据。

11.如权利要求10中所述的生物计量系统，其中所述对生物计量验证的请求包括用于会话密钥的种子，所述身份证明系统(110)包括被配置为在传送到所述身份验证系统(210)之前利用所述会话密钥将所述生物计量验证数据的至少一部分进行加密的加密单元，所述身份验证系统(210)包括被配置为对经加密的验证数据进行解密的解密单元。

12.一种生物计量方法(100)，包括

- 使用第一身体耦合通信接口(130)凭借身体耦合通信沿着或穿过个体传送生物计量验证数据到第二身体耦合通信接口，所述生物计量验证数据特定于所述个体的生物计量特征，所述生物计量验证数据被配置为对照从生物计量阅读器获得的生物计量数据来进行验证，所述生物计量阅读器被配置为测量所述个体的生物计量特征，所述生物计量验证数据包括生物计量助手数据以减少来自通过生物计量阅读器(220)获得的生物计量数据的噪声，生物计量阅读器(220)被配置为测量所述个体的生物计量特征。

13.一种生物计量方法(100)，包括

- 布置生物计量阅读器，使得在所述生物计量阅读器(220)对生物计量特征进行测量期间第二身体耦合通信接口接触或紧靠个体，以允许同时：

- 使用所述生物计量阅读器(220)测量所述个体的生物计量特征以获得生物计量数据，并且

- 使用所述第二身体耦合通信接口(230)凭借身体耦合通信沿着或穿过所述个体接收生物计量验证数据，所述生物计量验证数据包括生物计量助手数据以减少来自通过生物计量阅读器(220)获得的生物计量数据的噪声，生物计量阅读器(220)被配置为测量所述个体的生物计量特征。

14.一种存储计算机程序的计算机可读存储介质，所述计算机程序包括计算机程序代码模块，所述计算机程序代码模块适于当所述计算机程序在计算机上运行时执行权利要求12或13的所有步骤。

具有身体耦合通信接口的生物计量系统

技术领域

[0001] 本发明涉及生物计量系统，其包括被配置为测量个体的生物计量特征以获得生物计量数据(该生物计量数据遭受噪声)的生物计量阅读器，以及被配置为在生物计量验证数据的控制下将获得的生物计量数据映射到可再生生物计量数据从而减小来自生物计量数据的噪声的生物计量数据计量器。

[0002] 本发明进一步涉及一种生物计量方法和一种计算机程序。

背景技术

[0003] 生物计量学作为对很多安全问题的解决方案受到越来越多的关注。在生物计量学中，通过测量身体的一个或多个生物计量特征来识别人类。生物计量数据被称为是基于“他是谁”，而不是基于“他是什么”(例如智能卡)或“他知道什么”(例如口令)来识别人。

[0004] 使用生物计量系统，证人可向验证器识别或鉴定他自己。当使用生物计量系统来找出或检查人的身份时，存在两个选项：在识别中，证人的身份不是先验已知的，而是基于测量的生物计量特征，在数据库中执行搜索以找出匹配；在验证中，证人不仅允许他或她的生物计量特征的测量，还主张他或她的身份是什么。生物计量特征包括指纹、虹膜、视网膜、手掌等。

[0005] 然而，未解决的问题在于，当以大规模部署时，公民失去隐私，因为他必须将他的识别生物计量数据披露给他的银行、政府等。它们中的每个将获得相同测量数据，并且除非采取特别的预防措施，否则不保证这些方在任何时候都将不滥用生物计量数据来模仿该公民。

[0006] 在Jean-Paul Linnartz和Pim Tuyls的文章“New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates”中，介绍了生成用于在该方面上改进的函数的助手数据；该文章被进一步称为“Linnartz”。在登记阶段期间，证人佩吉(Peggy)接收包括生物计量助手数据和验证数据的生物计量模板。

[0007] 在使用阶段期间，佩吉允许维克托(Victor)得到她的生物计量特征X的可能有噪声的测量结果Y=X+N；N表示噪声。维克托在生物计量助手数据的控制下将获得的生物计量数据映射到可再生生物计量数据，以减少来自获得的生物计量数据的噪声。维克托然后应用密码学散列函数到可再生生物计量数据以获得输出U，将输出U与参考认证响应进行比较。在此，X、N和Y是实值或复值的矢量。

[0008] 来自O.Tochikubo等人的美国专利申请US2006/0274920描述了一种包括指纹传感器的个人识别设备以及用于验证的扫描器，该扫描器接收来自安装在佩戴在用户的手指、手腕或脚踝上的便携设备上的存储介质的指纹比较数据。S. Corroy等人的国际专利申请WO2010/064162A1描述了安全识别系统，其中用户通过佩戴在他/她身体上的识别设备或徽章或标签来获得访问权，其应用身体耦合通信(BCC)的技术来建立一种围绕该用户的电风。将身份证明(ID)经由BCC通信传送到安全识别系统的用户接口，并且由该系统通过基于该ID的假定安全BCC通信检查用户的身份的鉴定流程来鉴定该用户。

发明内容

[0009] 使用助手数据从获得的生物计量数据移除噪声允许密码学函数(如密码学散列函数)的使用;然而,其的确产生了在其被需要的地方处得到助手数据和/或验证数据的问题。尽管生物计量模板的使用可避免对于引用测量结果的大数据库(比如指纹数据库)的需求,但是其引入了对于使生物计量模板可用的新需求。可以以接触的方式(比如,存储在比如与生物计量特征的测量在时间上一起或接近地提供给卡阅读器的智能卡上)使生物计量模板可用。该途径是麻烦的;因为这对于用户而言意味着两个不同操作,在阅读器中加入卡并且提供他的生物计量特征用于测量。还可以从计算设备以非接触的方式(如无线地)使生物计量模板可用,但是这造成哪个无线信号属于哪个人的问题。此外,非接触卡等的使用不是那么吸引人,因为验证人将需要将该卡保持在他手中,这在他展示指纹的时候是笨拙的。

[0010] 将有利的是具有改进的生物计量系统。提供一种生物计量系统,其包括身份证明系统和身份验证系统。

[0011] 该发明涉及一种身份证明系统,该系统包括存储特定于个体的生物计量特征的生物计量验证数据的非易失性存储器,以及被配置为凭借身体耦合通信沿着或穿过个体的身体将生物计量验证数据传送到第二身体耦合通信接口的第一身体耦合通信接口。

[0012] 该发明还涉及一种身份验证系统,该系统包括被配置为测量个体的生物计量特征以获得生物计量数据的生物计量阅读器、被配置为凭借身体耦合通信沿着或穿过个体的身体接收生物计量验证数据的第二身体耦合通信接口(该生物计量阅读器被布置为使得第二身体耦合通信接口在通过生物计量阅读器对生物计量特征进行测量期间接触或紧靠该个体以允许所述接收)以及被配置为对照生物计量验证数据验证所获得的生物计量数据的生物计量数据验证器。身份验证系统可包括被配置为在生物计量助手数据的控制下将所获得的生物计量数据映射到可再生生物计量数据以便减少来自生物计量数据的噪声的生物计量数据计量器。

[0013] 身份证明系统包括存储用于个体的生物计量特征的生物计量验证数据的非易失性存储器,和被配置为凭借身体耦合通信沿着或穿过个体的身体将生物计量验证数据传送到第二身体耦合通信接口的第一身体耦合通信接口。身份验证系统包括被配置为测量个体的生物计量特征以获得生物计量数据的生物计量阅读器、被配置为凭借身体耦合通信沿着或穿过个体的身体接收生物计量验证数据的第二身体耦合通信接口(该生物计量阅读器被布置为使得第二身体耦合通信接口在通过生物计量阅读器对生物计量特征进行测量期间接触或紧靠该个体以允许该接收)、以及被配置为对照生物计量验证数据验证所获得的生物计量数据的生物计量数据验证器。

[0014] 身份验证系统包括被布置为使得第二身体耦合通信接口能够在生物计量阅读器正测量生物计量特征的同时接收身体间通信的生物计量阅读器和第二身体耦合通信接口两者。

[0015] 通过从证人系统发送验证数据到验证器系统,验证器系统可在被验证器信任的环境中执行验证(例如比较、匹配、近匹配等)。这在以下系统之上是优选的,在该系统中,如证人系统测量生物计量并且对照验证数据验证这些。这样的解决方案依赖于证人系统的完整性和硬件安全性,这通常在验证器系统的控制之外。

[0016] 生物计量验证数据被配置用于特定个体的特定生物计量特征，例如指纹或虹膜。生物计量数据验证器可以是生物计量信号处理器。如果生物计量数据验证器在对照所接收的生物计量验证数据验证所获得的生物计量数据中成功，则身份验证系统确认当前在生物计量阅读器之前的个体是被发放身份证明系统的同一个体，因此他的身份被验证。详细的实施例包含进一步的改进和细化。

[0017] 尽管这是非期望的，但是通常生物计量数据受到噪声或其它干扰。在一个实施例中，生物计量验证数据包括生物计量助手数据并且身份验证系统包括被配置为在生物计量助手数据的控制下减少来自所获得的生物计量数据的噪声的生物计量数据计量器。在对所测量的生物计量进行量化期间通过应用生物计量助手数据来减轻噪声或其它干扰的影响。优选地，将噪声的影响减轻到所获得的生物计量数据在所有或基本上所有的测量上是相同的程度。

[0018] 当已测量生物计量特征时，可通过应用助手数据来减轻固有噪声的影响。对于很多应用，无噪声的生物计量数据是优选的，但是实际上小的再现瑕疵通常是不可避免的，包括在身份证明应用中和在验证应用中。问题主要在人的生物计量值靠近量化边界时出现。于是小的瑕疵，少量的噪声可导致不同的数字表示。例如在'Linnartz'中实施助手数据的一个方式是将一个人的自然生物计量值移到量化间隔的中心。在这样的情况下，噪声非常不太可能改变在数字化之后的量化值。助手数据还可纯粹在数字域中起作用。示例是以下方案：一个人的生物计量是数字串，其中位错误可能发生。错误校正可能有帮助，但是仅在一旦生物计量的值碰巧与代码字(几乎)相同的时候。然而，一个人的生物计量本质上不等于特定代码字。然而，助手数据可将生物计量登记串转换(偏移或按位执行)成正好的代码字。如果在验证期间一些位错误出现，则错误校正可解码正确的代码字。在不具有助手数据的情况下，统计学上非常可能的是，人的生物计量位于两个代码字之间(比如在中间的某处)。然后随机位错误将使得解码器挑选相近的代码字中的任一个，但是没有任何保证其总是挑选到相同的代码字。助手数据可以被实施为将生物计量值从(数字)判定边界偏移开的偏置(bias)。在应用助手数据之后，生物计量数据更好地可再生并且允许密码学函数的使用。

[0019] 基于助手数据的噪声减小的另一优势是，其可加速在存储多个个体的多个预先测量的生物计量数据的数据库中对生物计量数据的查找。实际上，助手数据的一个特别应用是将生物计量数据库与所获得的验证串匹配。这比不具有助手数据的系统将需要寻找的近匹配快得多。而且，其易受在登记和验证期间的不同数字表示的侵害。

[0020] 当BCC被用作通信信道时，其避免对单独通信信道的需要。通过仅仅触摸与BCC接口组合的指纹阅读器，两个事项被同时建立：通过阅读器可以读取生物计量指纹并且获得BCC通信消息。

[0021] 此外，BCC减小在RF系统上/来自RF系统的干扰的影响，避免身体在无线电系统上具有的衰退效应，并且使能功率高效、高数据速率的无线链路。

[0022] 很多类型的生物计量阅读器要求在生物计量特征的测量期间对个体的身体的触摸。生物计量阅读器可要求触摸所针对的生物计量特征的示例包括指纹、手几何结构(手几何结构是通过他们的手的形状识别用户的生物计量)和手掌静脉辨识。其它生物计量阅读器可被实施为使得在测量期间要求触摸；例如虹膜或视网膜扫描器可被配置为使得用户放

置他的头从而他的面颊或下巴等触摸扫描器的参考壁或杯。这通过减小虹膜或视网膜的移动改进了扫描的精度，并且允许穿过被触摸的身体部分的身体耦合通信。

[0023] 包括可能的助手数据的生物计量验证数据是特定于生物计量特征并且特定于个体的。第一用户的虹膜扫描要求与第二用户的虹膜扫描不同的生物计量验证串和不同的助手数据。第一用户的虹膜扫描要求与第一用户的手掌扫描不同的生物计量验证数据。

[0024] 身体耦合通信(BCC)本身是已知的。已在例如Alberto Fazzi, Sotir Ouzounov, John van den Homberg的ISSCC 2009 / SESSION 11 / TD: TRENDS IN WIRELESS COMMUNICATIONS / 11.5, "A 2.75mW Wideband Correlation-Based Transceiver for Body-Coupled Communication"中描述了BCC。与人身体接触或紧靠的电子设备可使用其传导属性来建立在相互之间的身体耦合通信(BCC)。甚至在不具有直接皮肤接触的情况下，可经由电容式耦合到人身体的两个电极RX/TX设备实现BCC;TX生成可变电场，同时RX感测身体相对于环境的可变电势。

[0025] 在使用中，第一身体耦合通信接口将被布置用于与个体接触或紧靠地佩戴以允许与第二身体耦合通信接口的体内通信。个体一般是人个体，然而该系统还可有利地被应用于确认动物(如家禽，例如奶牛或马)。例如，可以将鼻纹用作生物计量以识别牲畜，或可将在啮齿动物的耳朵中的血管图案用作生物计量。

[0026] 两个BCC接口与个体的身体接触或紧靠以允许在这两个接口之间穿过身体的通信耦合。一些研究者解析了，与"穿过"身体相对，通信信号沿着或者经由身体的表面行进。但对于本发明，精确解释不那么相关，只要信号在身体的紧邻处足够强并且可良好接收，优选地但不一定通过触摸传递。通常，比起EM无线电通信波，BCC信号随着与身体的距离增大而衰减得更快。除了电场BCC，可被用于我们的生物计量验证目的的BCC的其它变型包括但不限于，磁耦合，因为其例如被已知用于助听器中以在附接到两个耳朵的两个助听器之间通信。

[0027] 在一实施例中，身份证明系统的非易失性存储器和第一身体耦合通信接口被包括在同一设备中;例如，被配置成佩戴例如在臂带、腿带、腕表等中的单一身体标签。在一实施例中，身份验证系统的至少生物计量阅读器和第二身体耦合通信接口被包括在同一设备中;例如，单一生物计量阅读设备。身份证明系统与身份验证系统不同。

[0028] 在一实施例中，身份证明系统包括被配置为穿过个体的身体传送生物计量验证(助手)数据到身份验证系统的控制逻辑。

[0029] 在一实施例中，验证数据包括控制生物计量数据，已预先通过测量个体的生物计量特征获得控制生物计量数据，生物计量数据验证器被配置为对照控制生物计量数据来验证所获得的生物计量数据。例如，可以通过对差异的数量进行计数来对照控制生物计量数据验证所获得的生物计量数据，如果该数量小于验证阈值，则身份被验证。

[0030] 在一实施例中，验证数据包括验证码，通过应用密码学单向函数到控制生物计量数据来预先获得所述验证码，已通过测量个体的生物计量特征预先获得控制生物计量数据，生物计量数据验证器被配置为应用密码学单向函数到所获得的生物计量数据来获得候选验证码并且被配置为测试候选验证数据是否等于验证码。

[0031] 如果候选验证码等于验证码，则验证了生物计量验证数据的确匹配该个体。取决于单向函数的密码学属性，可以得出不同的结论，例如如果单向函数是消息鉴定函数(比如

带有密钥的散列函数)，则可以推断出，生物计量验证数据通过知道该密钥的实体发出。注意，与签名和信任机制的组合可相当大地加强可得出的结论。信任机制可以仅仅是存储在阅读器处的公钥，但还可以是例如链接到签名权力机构的证书等。

[0032] 助手数据和验证码的组合是特别有利的。其避免生物计量控制数据的公开，还不要求数据库。

[0033] 在稍微不同的实施例中，验证数据不包含助手数据，而仅仅是生物计量值的加密形式，由于其是在登记个体时测量的。验证系统知道解密密钥，并且获取生物计量登记数据。验证系统还测量候选者的实际生物计量。如果实际值和登记值“充分相等”，则验证系统接受该候选者是真实的。在此“充分相等”暗指，在实际和登记数据之间的微小差别归因于噪声或其它干扰，但是不被视为取消候选者资格的理由。例如，可以要求的是，在实际值和登记值之间的可能的加权汉明距离小于阈值。阈值可以是预先确定的。阈值可取决于实际应用。如果同一系统被用于高安全应用，则可使用小阈值，接受偶然的错误否定(false negative)以交换较高的安全性；对于低安全应用，可使用高阈值，接受偶然的错误肯定(false positive)以交换较高的用户友好度。

[0034] 在一实施例中，第一身体耦合通信接口被配置为穿过个体的身体将用于应用中的个体的身份数据传送到第二身体耦合通信接口，第二身体耦合通信接口被配置为穿过个体的身体接收身份数据，并且身份验证系统包括身份输出单元，身份输出单元被配置为如果候选验证数据等于验证数据，则将身份数据转发给应用，以及如果候选验证数据不等于验证数据，则不将身份数据转发给应用。

[0035] 该应用可以是软件应用。例如生物计量系统可被用于入口控制。该应用验证该身份是否被允许进入特定房间、建筑物等。

[0036] 在一实施例中，第一身体耦合通信接口被配置为穿过个体的身体将数字签名传送到第二身体耦合通信接口，第二身体耦合通信接口被配置为穿过个体的身体接收数字签名。身份验证系统包括被配置为验证数字签名的数字签名验证器，其中数字签名对生物计量验证数据中的所有或至少一部分(优选地还有身份数据和可选地还有助手数据)进行签名。

[0037] 数字签名优选是对应于公共、私有密钥对的非对称数字签名。非对称数字签名具有可通过知道该密钥对的公钥的任何人来验证的属性，但是仅可由知道该密钥对的私钥的某人做出。这具有令人关注的优势，身份验证系统仅需要访问公钥对来进行验证，因此一种折衷的身份验证系统不包括在生物计量系统中的其它身份验证系统。例如，可以在登记阶段期间，比如通过某一权力机构来对生物计量模板和/或身份进行签名。该权力机构还可确定生物计量模板，即生物计量助手数据和生物计量验证数据。

[0038] 在一实施例中，个体的生物计量特征是个体的指纹并且生物计量阅读器是指纹阅读器。测量指纹暗含了手指的接触，因此在该测量发生时可方便地完成BCC通信。

[0039] 在一实施例中，第二身体耦合通信接口被配置为穿过个体的身体传送对生物计量验证的请求到第一身体耦合通信接口。身份证明系统被配置为响应于穿过个体的身体接收对生物计量验证的请求来传送生物计量验证数据。这样的通信触发允许身份证明系统的大多数在大多数时间休眠，因此节省能量。在该情况下，用户的触摸完成三件事情：生物计量验证请求充当通信触发，测量生物计量特征，以及用于传送生物计量数据(例如生物计量助

手数据、验证数据、身份数据和签名数据中的一个或多个)的通信信道。

[0040] 在一实施例中,对生物计量验证的请求包括用于会话密钥的种子。身份证明系统包括加密单元,加密单元被配置为在传送到身份验证系统之前利用会话密钥对生物计量验证数据的所有或至少一部分进行加密。身份验证系统包括被配置为对经加密的验证数据进行解密的解密单元。

[0041] 可以直接使用该种子用于加密通信。身份证明系统和身份验证系统还可采用密钥协商协议,例如Diffie-Helman或其的某种变型,其中身份证明系统可利用另外的种子响应,在此之后,身份证明系统和身份验证系统都计算出相同的会话密钥。身份证明和验证系统可包括随机数生成器来共同生成会话密钥。

[0042] 身份证明系统可以是所谓的标签。标签一般大规模生产,然而需要少得多的阅读器。例如,身份证明系统可以是用于公共运输旅行者的标签卡。身份验证系统可以是接入端口,比如到平台的接入端口。可通过若干不同制造商生产标签和/或阅读器。

[0043] 身份证明系统和身份验证系统是电子设备。身份证明系统是移动电子设备,其可包括电池。

[0044] 本发明的一方面涉及由身份证明系统使用的生物计量方法。一种方法包括使用第一身体耦合通信接口凭借身体耦合通信沿着或穿过个体的身体传送生物计量验证数据到第二身体耦合通信接口,该生物计量验证数据特定于个体的生物计量特征,例如生物计量助手数据被配置为控制由生物计量数据计量器将受到噪声的生物计量数据映射到可再生生物计量数据,从而减少来自生物计量数据的噪声的影响。从与个体的身体接触或紧靠的第一身体耦合通信接口将生物计量验证数据传送到与个体的身体接触或紧靠的第二身体耦合通信接口。

[0045] 本发明的一方面涉及由身份验证系统使用的生物计量方法。一种方法包括布置生物计量阅读器,使得在生物计量阅读器对生物计量特征进行测量期间第二身体耦合通信接口与个体接触或紧靠,以允许使用第二身体耦合通信接口凭借身体耦合通信沿着或穿过个体的身体接收生物计量验证数据,并且使用生物计量阅读器测量个体的生物计量特征以获得生物计量数据。生物计量阅读器和第二身体耦合通信接口可以被包括在单个设备中,如在集成的身份验证系统中。

[0046] 根据本发明的方法可以在计算机上被实施为计算机实施的方法,或在专用硬件中实施,或以两者的组合实施。根据本发明的方法的可执行代码可以被存储在计算机程序产品上。计算机程序产品的示例包括存储器设备、光学存储设备、集成电路、服务器、在线软件等。优选地,计算机程序产品包括存储在计算机可读介质上的非暂时性程序代码模块,其用于当所述程序产品在计算机上执行时执行根据本发明的方法。

[0047] 在优选实施例中,计算机程序包括适于当计算机程序在计算机上运行时执行根据本发明的方法的所有步骤的计算机程序代码模块。优选地,计算机程序在计算机可读介质上具体体现。

[0048] 参考所谓的卡上匹配系统,参见例如NIST Interagency Report 7452,'Secure Biometric Match-on-Card Feasibility Report',第二页。卡上匹配的情形如下:持卡者向非接触生物计量阅读器呈现他们的卡。持卡者向生物计量扫描器呈现他们的手指。主机建立与该卡的安全会话。主机准备经加密的指纹(图像或细目)并且经由非接触接口将其传

送到卡。卡解密该模板并且将其与存储在卡上的参考模块比较。卡返回签名的结果(即是/否)给主机。

[0049] 在卡上匹配系统中,从阅读器将测量的指纹传送到卡,从而所有计算需要在卡上完成,这暗含了在卡处需要更多资源。将期望的是,替代在卡上,在阅读器上执行计算密集操作。卡上匹配系统不允许主机控制生物计量的匹配,然而通过传送生物计量模板到主机,主机确实控制该匹配,同时避免一个人的生物计量特征数据的不加选择的广播。

附图说明

[0050] 根据下文描述的实施例,本发明的这些和其它方面将显而易见,并且将参考下文描述的实施例来阐明本发明的这些和其它方面。在图中,

[0051] 图1示出生物计量系统100的正视图,

[0052] 图2示出生物计量系统100的框图,

[0053] 图3示出图示了登记方法300的流程图,

[0054] 图4示出图示了生物计量方法400的流程图。

[0055] 应当注意到,在不同图中具有相同附图标记的项目具有相同的结构特征和相同的功能,或是相同的信号。在已经解释了这样的项目的功能和/或结构的情况下,在详细描述中没有必要对其进行重复解释。

[0056] 图1-2中的附图标记的列表

[0057] 110 BCC标签

[0058] 210 鉴定系统

[0059] 250 BCC信道

[0060] 260 个体

[0061] 120 控制逻辑

[0062] 125 存储器

[0063] 130 BCC接口

[0064] 220 生物计量阅读器

[0065] 230 BCC接口

[0066] 242 生物计量数据计量器

[0067] 244 生物计量数据验证器

[0068] 246 身份输出单元

[0069] 248 数字签名验证器。

具体实施方式

[0070] 尽管本发明容许很多不同形式中的实施例,但是在具有以下理解的情况下,在图中示出并且本文将详细描述一个或多个具体实施例:本公开应当被认为是本发明的原理的例示,并且非旨在将本发明限制到所示出和描述的具体实施例。

[0071] 图1和2图示了生物计量系统100。该系统包括在此以BCC标签110的形式的身份证明系统和在此以鉴定系统210的形式的身份验证系统210。

[0072] 在该情况下,身份证明系统110是身体佩戴的包含数据的识别设备。身份证明系统

110包括控制逻辑120、存储器125和BCC接口130。如示出的BCC标签被集成在个体佩戴的腕表中，这提供标签与个体的皮肤的直接接触。腕表是一种佩戴BCC标签的示例性方式。也可以使用弹性带或胶水等将BCC标签保持靠近皮肤。

[0073] 身份验证系统210包括第二BCC接口230。在身份证明系统110和身份验证系统210之间的是BCC信道250。BCC信道是穿过个体的身体运行的通信信道。在系统100的情况下，信道穿过在使用系统100的图1中示出的个体260的手和手指运行。该信道由身份证明系统110中的第一BCC接口130和身份验证系统210中的第二BCC接口230形成。BCC接口130和230可包括两个电极，即接收电极(RX)和发射电极(TX)。两个电极可电容式耦合到该个体的人体；TX生成可变电场同时RX感测身体关于环境的可变电势。第一BCC接口130被至少配置为发送数据并且第二BCC接口230被至少配置为接收数据；然而在更高级的实施例中，第一BCC接口130和第二BCC接口230都被配置为发送和接收数据。

[0074] 可佩带电子标签110在存储器125中存储个体的识别数据。存储器125存储生物计量验证数据(包括生物计量助手数据)，但是还可存储任何其它验证数据、身份数据和在该数据上的签名。在一个实施例中，身份数据和/或签名数据是缺失的。生物计量验证数据(包括验证码)、身份数据和签名是例如在登记阶段期间，针对图1中示出的个体260特别计算的并且被存储在存储器125中。

[0075] 应注意到，生物计量助手数据并非是必须的，例如可存储生物计量控制数据。在那种情况下，将获得的生物计量数据直接与生物计量控制数据比较，这考虑可能出现的噪声和其它干扰。优选地，当使用助手数据时，还使用验证码。

[0076] 在系统100的一个实施例中，身份证明系统110通过身体耦合的身体通信，连续广播生物计量验证数据以及可能地，其它数据(例如个体标识符)。在那种情况下，一旦个体与目标设备接触，身份证明系统110就传送身体耦合通信，从而通信式耦合是可能的。替代地，身份证明系统110当其接收到如此做的触发时，才传送存储在存储器125中的数据。触发可来自系统210，但还可来自不同的源；例如，个体260可以给出触发，例如通过按压在系统110上的按钮。

[0077] 身份验证系统210包括用于测量个体260的生物计量特征的生物计量阅读器220。在如示出的系统中，生物计量特征是指纹。还便利的是手几何结构扫描器和手掌静脉扫描器。有点不那么便利但是仍然对于系统100可充分修正的是虹膜和视网膜扫描器等，其中与身体的接触不是要求的，但是其中，在生物计量测量期间可容易布置这样的接触。

[0078] 已经在身份验证系统210中布置生物计量阅读器220和第二BCC接口230，从而当个体260使用生物计量阅读器220来使其生物计量特征被测量时，他自动建立所要求的在他身体与第二BCC接口230之间的通信式耦合，以及因此在第一BCC接口130和第二BCC接口230之间的通信式耦合。这意味着在测量生物计量特征的时候，可同时交换数据。在测量(扫描期间)，控制逻辑120经由第一BCC接口130，至少发送从存储器125获取的生物计量验证数据到第二BCC接口230。

[0079] 身份验证系统210还包括生物计量数据计量器242(还被称为生物计量映射器)以在经由BCC信道250从身份证明系统110获取的生物计量助手数据的控制下将从生物计量阅读器220获得的生物计量数据映射到可再生生物计量数据。该映射减小了来自生物计量数据的噪声的影响，特别是例如通过增大所测量的数据位于接近的数字代码字的量化间隔的

中心附近的概率，使数据更好地可再生。将结合图3和4在下文描述做出并且应用生物计量助手数据的一个方式。

[0080] 在一些实施例中，直接使用校正噪声后的生物计量数据来在数据库中查找数据，简化了该系统。在具体实施方式的剩余部分中，将假定生物计量数据已被配置为完全去除噪声并且使用验证码。注意，在具有高噪声的异常环境中，该系统可能仍然无法确保测量结果落入相同间隔中；这可导致系统的偶然故障。此情况的可能性可通过使用更大的定量间隔、错误校正、执行第二验证尝试等来减小。

[0081] 身份验证系统210可进一步包括被配置为应用密码学单向函数到可再生生物计量数据以获得候选验证码的生物计量数据验证器244。密码学单向函数可以是密码学散列函数，如SHA-1或MAC，如带有密钥的散列，如HMAC-SHA1。生物计量数据验证器244被另外配置为测试候选验证码是否等于经由BCC信道250从身份证明系统110接收的验证码。

[0082] 身份验证系统210可进一步包括身份输出单元246，假如生物计量数据验证器244中的测试成功的话，即当验证码等于候选验证码的时候，身份输出单元246转发经由BCC信道250接收的身份数据并且向应用(如软件应用)标识个体260。可以在使用例如输出所接收的身份之前的任意点进行签名的验证。例如，系统210可甚至在校正生物计量数据之前验证签名。

[0083] 身份验证系统210可进一步包括数字签名验证器248。数字签名验证器248验证经由BCC信道250接收的数字签名。例如，数字签名可以是非对称签名，例如RSA签名或ECDSA签名，其签名于经由BCC信道250接收的数据，例如生物计量数据、验证码和身份数据。

[0084] 图3图示了准备身份证明系统110用于使用(所谓的登记)的方法。在步骤310中，对系统使用的生物计量特征(在系统100的情况下，是指纹)进行测量。生物计量数据可以以矢量数字数据的形式。在步骤320中，针对所测量的生物计量数据来计算生物计量助手数据。在可选步骤330中，产生验证码。这可通过首先计算可再生生物计量数据来完成，可再生生物计量数据将通过应用步骤320的生物计量助手数据到步骤310的生物计量数据来获得。应用密码学单向函数(如散列)到可再生生物计量数据。可能需要中间处理，如矢量的串联、填补等。在可选的步骤340中，获得，如查询，或从电子系统(如电子护照)读出身份数据。所获得的数据，即生物计量助手数据、验证码和身份数据被数字化签名以产生数字签名。注意，假定是可分离的签名，但其不是必需的，例如数据和签名可被组合。最终在步骤360中，将生物计量助手数据、验证码、身份数据和签名存储在身份证明系统110的存储器125中。注意，既不将生物计量数据也不将可再生生物计量数据存储在身份证明系统110上。(可再生)生物计量数据甚至是不能仅从存储在存储器125中的数据得到。有趣地，即使可再生生物计量数据未被存储在存储器125中，但是可将可再生生物计量数据包括在经由其计算签名的数据中；这假定了可分离签名。当可再生生物计量数据被包括在签名中，但不在从系统110传输到系统210的数据中时，甚至可省去验证码，因为签名的验证已经提供了生物计量对应于BCC标签的保证。可分离签名可与其所签名的数据分离，并且不允许所签名的数据被重构。

[0085] 不具有验证码的实施例的示例是一种生物计量系统，其包括身份证明系统和身份验证系统，该身份证明系统包括用于存储生物计量鉴定数据的非易失性存储器和第一身体耦合通信接口，该生物计量鉴定数据包括针对个体的特定生物计量特征的生物计量助手数据和数字签名，该数字签名对至少生物计量助手数据和可再生生物计量数据进行了签名，

该第一身体耦合通信接口被配置为穿过个体的身体将生物计量鉴定数据传送到第二身体耦合通信接口；该身份验证系统包括被配置为测量个体的生物计量特征以获得生物计量数据(该生物计量数据受到噪声)的生物计量阅读器、第二身体耦合通信接口、生物计量数据计量器和数字签名验证器，该第二身体耦合通信接口被配置为通过个体的身体接收生物计量鉴定数据，生物计量阅读器被布置为使得第二身体耦合通信接口在通过生物计量阅读器对生物计量特征进行测量期间与个体接触或紧靠个体以允许该接收，生物计量数据计量器被配置为在来自所接收的生物计量鉴定数据的生物计量助手数据的控制下将所获得的生物计量数据映射到可再生生物计量数据从而减少来自生物计量数据的噪声，数字签名验证器被配置为至少经由来自所接收的生物计量鉴定数据的生物计量助手数据和通过生物计量数据计量器获得的可再生生物计量数据来验证来自所接收的生物计量鉴定数据的数字签名。

[0086] 图4图示了可使用身份证明系统110和身份验证系统210的生物计量方法400。在步骤410中，通过第二身体耦合通信接口230，如通过身份验证系统210，传送对生物计量验证的请求。在步骤420中，在第一身体耦合通信接口130，如通过身份证明系统110接收对生物计量验证的请求。步骤410和420是可选的，例如身份证明系统110可连续广播生物计量验证数据。响应于该请求(如果使用请求的话)，在步骤430中，通过第一身体耦合通信接口，例如通过身份证明系统110来传送生物计量验证数据。

[0087] 在步骤440中，使用第二身体耦合通信接口230接收生物计量助手数据并且在步骤450中，使用生物计量阅读器来测量个体的生物计量特征以获得生物计量数据。步骤440和450是基本上平行的，即同时发生或至少具有大的重叠，或步骤440和450之一在时间上与另一个重叠。因此，获得生物计量助手数据和生物计量数据两者所需的时间量小于通过一个接一个地接收所需要的时间量。即使步骤440和450不重叠，仍然避免了第二通信信道(例如非接触卡)。

[0088] 在步骤460中，对照生物计量验证数据来验证所获得的生物计量数据以验证身份。如果生物计量助手数据被包括在生物计量验证数据中，则通过生物计量数据计量器在生物计量助手数据的控制下将所获得的生物计量数据映射到可再生生物计量数据，从而去除来自生物计量数据的噪声。

[0089] 可以以多种方式使用可再生生物计量数据。例如，可在生物计量数据的数据库中查找它。或可利用密码学操作(例如如本文描述的)来进一步处理它。密码学操作具有这样的属性：输入中的甚至一位的差别通常都具有很大差异的输出。为此原因，这样的密码学的使用可能需要可再生生物计量数据。

[0090] 下文给出了实施生物计量助手数据和验证码的一种方式。其它选项是可能的。

[0091] 当个体260针对生物计量验证系统进行登记时，测量个体260的生物计量特征(如指纹)X。在此，X是具有一些干扰的表示。通过量化函数Q来量化该指纹，如Z=Q(X)，使得Z描述X所处的量化间隔的中间。例如，X可以是矢量，并且可量化该矢量的每个分量。

[0092] 量化函数将高分辨率变量(如矢量分量)映射到较低分辨率变量。例如，可通过跨越分量的域的一系列间隔来定义Q。该分量所处的间隔的中心是该分量的量化值。在量化之后，通常相当大地减小了变量可呈现的不同值的数量。而且，在量化之后，变量位于量化间隔的中心处。

[0093] 登记系统计算两个值，助手数据W=X-Q(X)，和验证码S=Hash(Q(X))。如从个体260的护照获得身份数据P。登记系统然后通过添加证书和签名C来对数据串[W, S, P]进行签名。证书是可选的。值W、S、P、C例如作为串联的串被存储在BCC标签110中，其被给予个体260。

[0094] 个体260现在准备好在验证系统中(例如身份验证系统210)中证明他的身份。

[0095] 身份验证系统210测量生物计量特征，即指纹X'，和经由身体耦合通信信道250接收的数据W、S、P、C。其检查签名C是否对于W、S、P有效。如果签名无效，则该过程终止，可能采取适当的动作，例如引发错误。甚至在无效签名的情况下也保持通过生物计量阅读器220获得的生物计量数据。无效签名可指示利用设备的非法篡改；指纹可被用作证据。

[0096] 接着，验证系统计算X'-W，并且利用Q来量化它，并且散列它。换言之，验证系统计算S'=hash(Q(X'-W))并且检查是否S=S'。如果S=S'，则其接受佩吉具有如在P中描述的身份。在此，函数Q(X-W)是δ (delta)收缩函数G(X,W)。其它δ收缩函数是可能的，参见例如Linnartz和涉及该文章的公开物。

[0097] 注意，验证器获得 Q(X'-W) = Q (X'-(X-Q(X))) = Q((X'- X) + Q(X))。因为Q(X)位于量化间隔的中心并且(X'-X)是小的，即在噪声的级中，Q((X'- X) + Q(X))很可能等于Q(X)。还注意，W未给出关于X或Q(X)的信息。

[0098] 典型地，设备110和210各自都包括执行在设备110和210处存储的适当软件的微处理器(未单独示出)，例如该软件可能已经被下载并且存储在对应的存储器(未示出)中。

[0099] 对于本领域技术人员来说将明显的是，执行如本文描述的生物计量方法的很多不同方式是可能的。例如，步骤的顺序可以是变化的或一些步骤可以并行执行。而且，在步骤之间，可以插入其它方法步骤。插入的步骤可表示如在本文中描述的方法的细化，或可与该方法不相关。例如，步骤330和340或步骤440和450可以被至少部分并行地执行。而且，在开始下一步骤之前，给定的步骤可能未完全完成。

[0100] 可使用软件来执行根据本发明的方法，该软件包括用于使得处理器系统执行方法300或400的指令。软件可以仅包括由系统(例如系统110或210)的特定子实体采取的那些步骤。软件可被存储在适当存储介质(例如硬盘、软盘、存储器等)中。可以将软件作为沿着缆线或无线的信号进行发送，或可以使用数据网络(例如互联网)来发送软件。可以使得软件可用于下载和/或用于服务器上的远程使用。

[0101] 将认识到，本发明还扩展到适于将本发明投入实践的计算机程序，特别是在载体上或中的计算机程序。程序可以是源代码、目标代码、介于源和目标代码之间的代码(比如部分编译的形式)的形式，或适合在根据本发明的方法的实施中使用的任何其他形式。涉及计算机程序产品的实施例包括对应于陈述的方法中的至少一个方法的处理步骤中的每个的计算机可执行指令。这些指令可被细分为子例程和/或被存储在可静态或动态链接的一个或多个文件中。涉及计算机程序产品的另一实施例包括对应于陈述的系统和/或产品中的至少一个中的模块中的每个的计算机可执行指令。

[0102] 应当注意到，上文提到的实施例说明而非限制本发明，并且本领域技术人员将能够设计很多替代实施例。

[0103] 在权利要求中，被放置在括号之间的任何附图标记不应当被解释为限制权利要求。动词“包括”及其词形变化的使用不排除除了在权利要求中陈述的那些元件或步骤之外

的元件或步骤的存在。在元件之前的冠词“一”或“一个”不排除多个这样的元件的存在。可凭借包括几个不同元件的硬件，并且凭借适当编程的计算机来实施本发明。在枚举几个模块的设备权利要求中，可通过一个并且同一项硬件来具体体现这些模块中的几个。在相互不同的从属权利要求中记载某些措施的单纯事实不表明这些措施的组合不能被有利地使用。

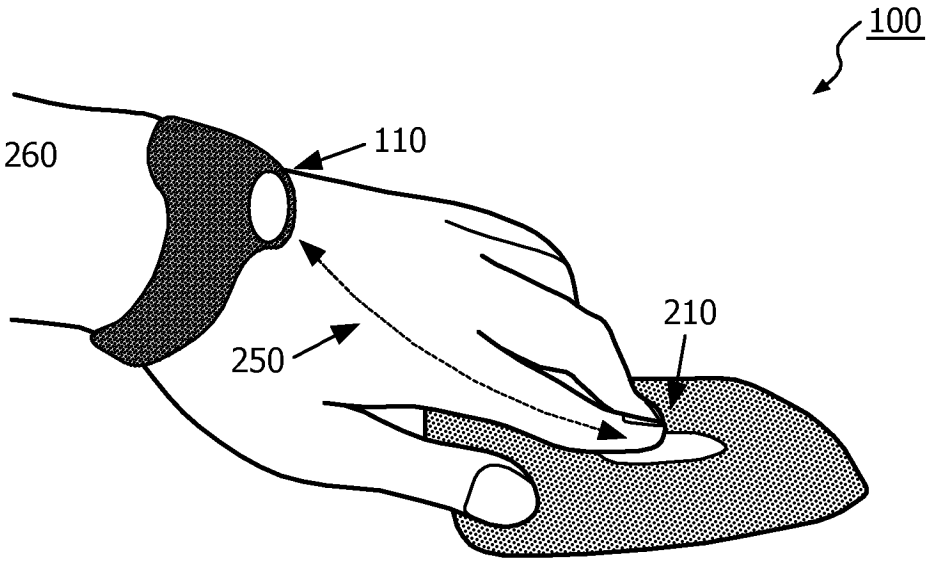


图 1

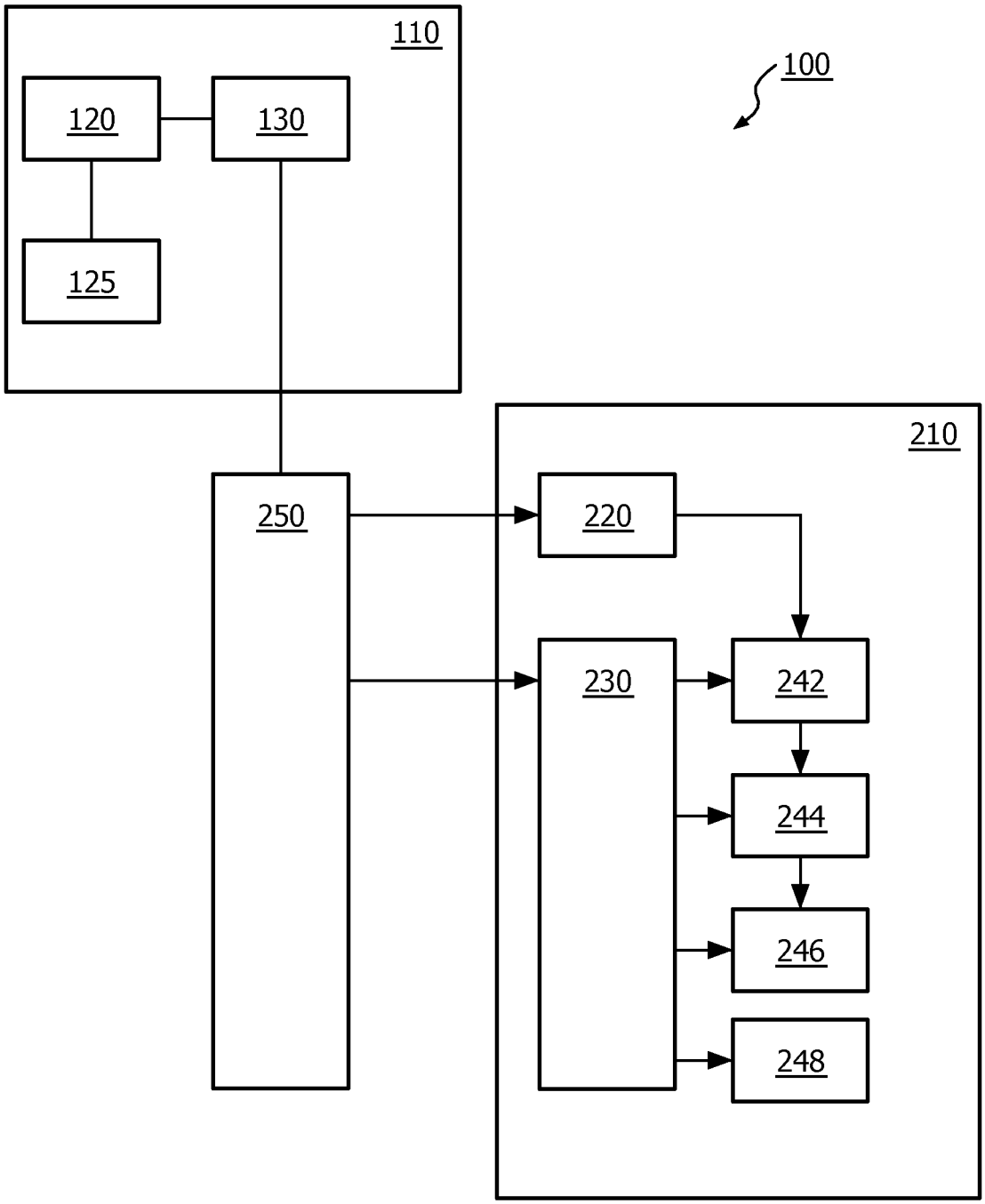


图 2

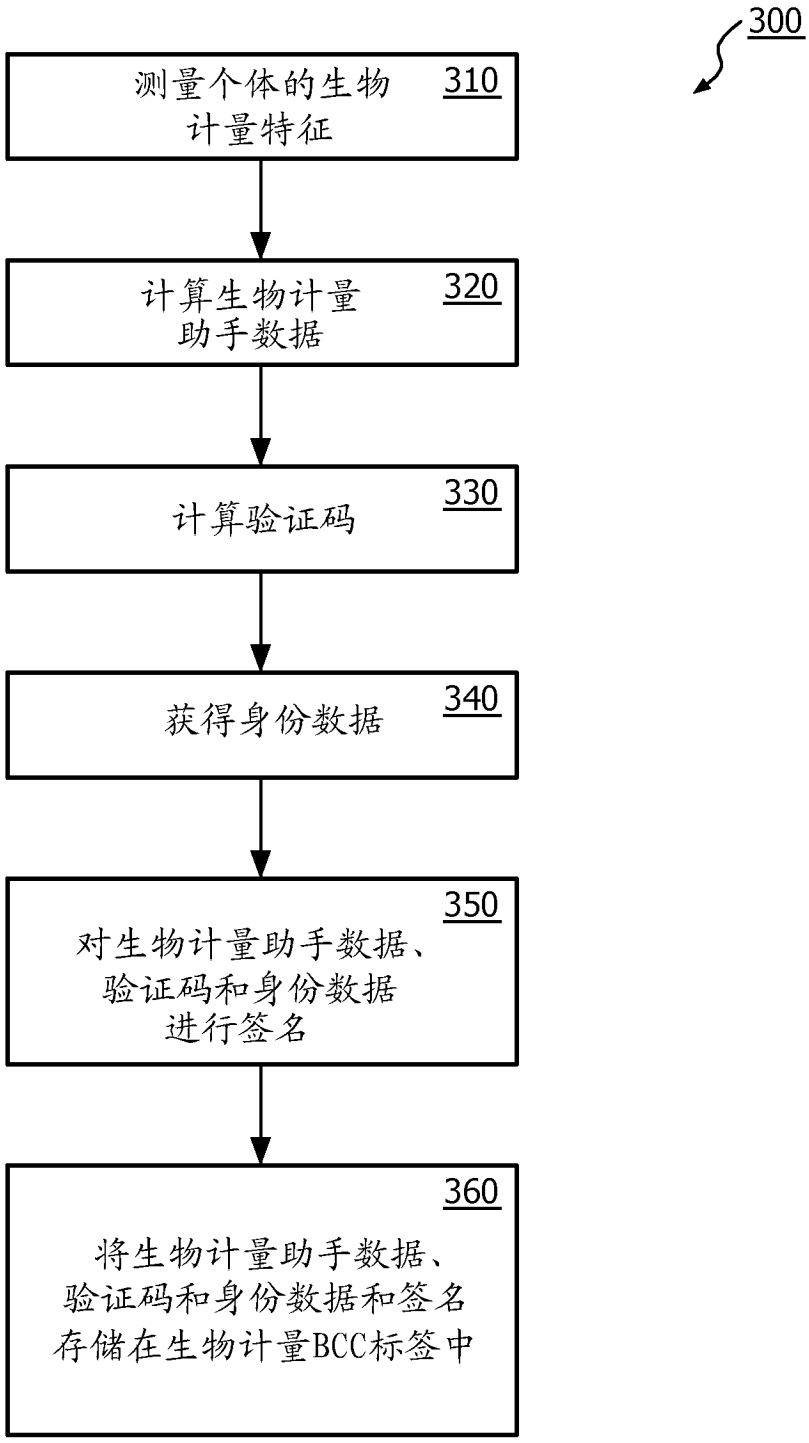

300
测量个体的生物计量特征
310
计算生物计量助手数据
320
计算验证码
330
获得身份数据
340
对生物计量助手数据、验证码和身份数据进行签名
350
将生物计量助手数据、验证码和身份数据和签名存储在生物计量BCC标签中
360

图 3

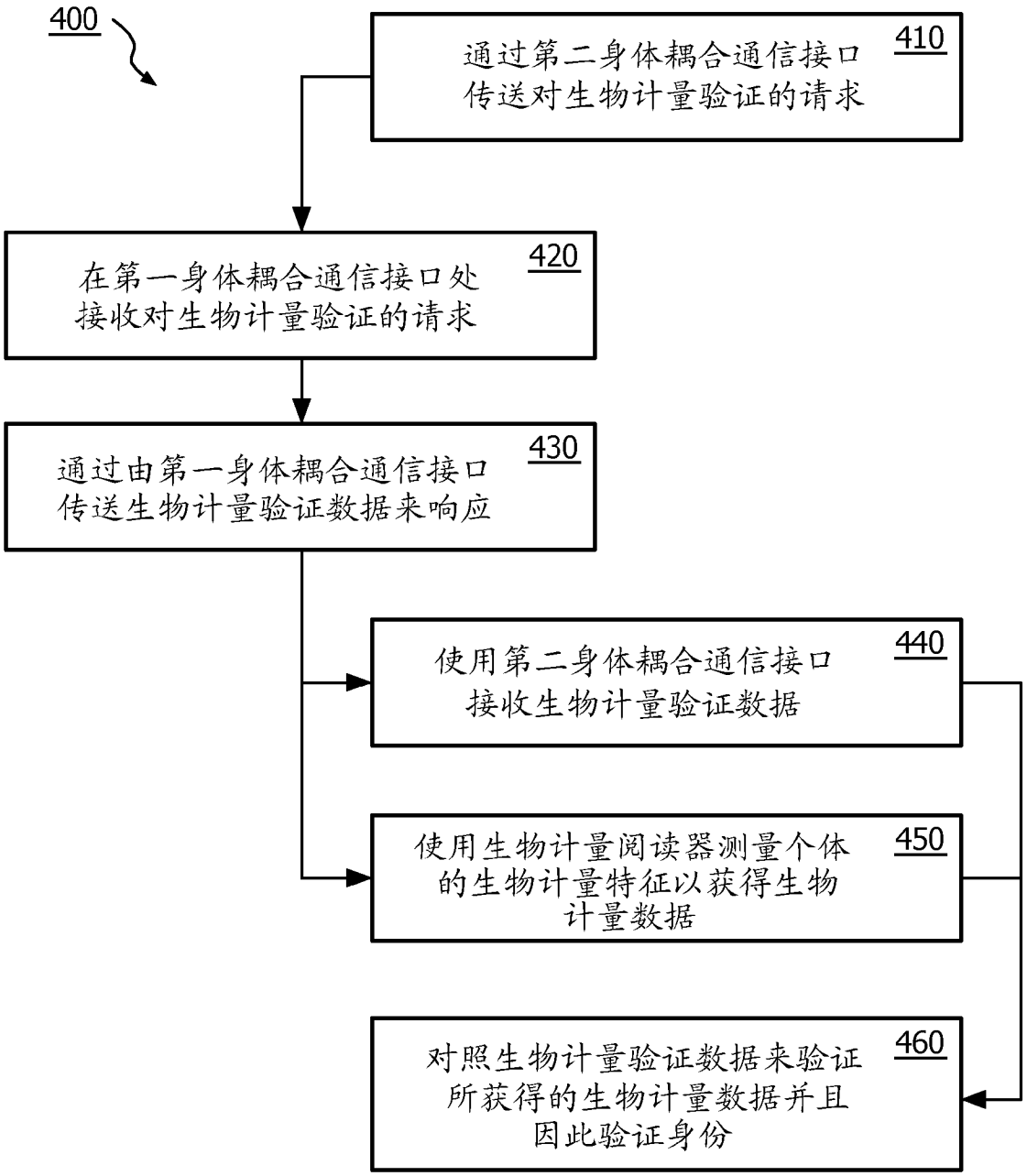

400
410
通过第二身体耦合通信接口
传送对生物计量验证的请求
420
在第一身体耦合通信接口处
接收对生物计量验证的请求
430
通过由第一身体耦合通信接口
传送生物计量验证数据来响应
440
使用第二身体耦合通信接口
接收生物计量验证数据
450
使用生物计量阅读器测量个体
的生物计量特征以获得生物
计量数据
460
对照生物计量验证数据来验证
所获得的生物计量数据并且
因此验证身份

图 4